AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended): A method of ~~authorising~~ authorizing a user device of a key and lock system, wherein said user device is a user key or a lock of a master key system, wherein the master key system enables various persons with different access authorizations to access all relevant items with only one key, the method comprising the following steps:

creating said user device having an electronic circuitry comprising an electronic code memory and being arranged to carry out software operations,

creating a first system device having an electronic circuitry and being used in a first level of said key and lock system,

storing a first encryption key in said user device and said first system device,

carrying out an authentication process between said user device and said first system device using said first encryption key, and

in case said authentication process was successful, carrying out a software operation by said first system device, by which software operation said encryption key stored in said first user device is replaced by a second encryption key,

wherein said second encryption key is stored in second system devices and further user devices used in a second level of said key and lock system, thereby making said user device operable with said second system and further user devices, and

wherein, also during the authentication process, said electronic encryption keys in the system devices and first and further user devices are unreadable from outside said electronic circuitry and only used by algorithms executed internally ~~of~~ in the user device and wherein, when an encryption key used by the algorithms internally in the user device result in the successful authentication, the encryption key is replaced with another key of a different level.

2. (previously presented): The method according to claim 1, wherein, during the step of replacing said first encryption key stored in said user device, said second encryption key is supplied by said first system device.

3. (previously presented): The method according to claim 1, wherein, during the step of replacing said first encryption key stored in said user device, said second encryption key is supplied by a computer.

4. (original): The method according to claim 3, comprising the additional step of supplying said second encryption key to said computer through a network including local networks and public telephone networks.

5. (previously presented): The method according to claim 1, wherein said first system device is a system key of a master key system, wherein the master key system enables various persons with different access authorizations to access all relevant items with only one key.

6. (previously presented): The method according to claim 1, wherein said user device is a user key of a master key system, wherein the master key system enables various persons with different access authorizations to access all relevant items with only one key.

7. (previously presented): The method according to claim 1, wherein said user device is a lock of a master key system.

8. (canceled).

9. (currently amended): An electromechanical key and lock device of a master key system, wherein the master key system enables various persons with different access authorizations to access all relevant items with only one key, said key and lock device comprising:

an electronic circuitry having an electronic memory adapted for storing an electronic code and being arranged to carry out software operations, said electronic code uniquely identifying the device and comprising a first electronic encryption key,

wherein said first encryption key being adapted to be replaced by a second encryption key by means of an authenticated software operation carried out by a first system device having said first encryption key and being used in a first level of a lock system, and

said second encryption key is stored in system and user devices used in a second level of said lock system, thereby making said user device operable with said second system and user devices, and

wherein, also during the authentication process, said electronic encryption key stored in the system and user devices are unreadable from outside said electronic circuitry and only used by algorithms executed internally of the key and lock device and wherein, when the electronic encryption key used by the algorithms executed internally of the key and lock device result in the successful authentication, the electronic encryption key is replaced with another key of a different level.

10. (original): The device according to claim 9, wherein said first system device is a key having a programmable electronic circuitry.

11. (original): The device according to claim 9, wherein said electronic encryption keys are unreadable from outside said electronic circuitry.

12. (currently amended): A key and lock master key system, wherein the master key system enables various persons with different access authorizations to access all relevant items with only one key, said system comprising:

a plurality of user devices comprising:

a plurality of user keys having an electronic circuitry comprising an electronic memory adapted for storing a variable electronic encryption key and being arranged to carry out software operations, and

a plurality of locks having an electronic circuitry comprising an electronic memory adapted for storing a variable electronic encryption key,

wherein a user key and a lock are operable only if there are stored identical encryption keys in said user key and the lock,

at least one system device having an electronic circuitry comprising an electronic memory adapted for storing a permanent electronic encryption key, and

a computer program software adapted to change the variable electronic encryption key of a user device from a first to a second encryption key as a result of a successful authentication process carried out between

a lock or user key having a stored variable electronic encryption key, and

a system device having an identical encryption key as said lock or user key,

wherein said second encryption key is stored in second system devices and user devices used in a second level of said key and lock system, thereby making said user devices operable with said second system and user devices, and

wherein, also during the authentication process, said electronic encryption keys in the system and user devices are unreadable from outside said electronic circuitry and only used by algorithms executed internally ~~of~~ in the user devices and wherein, the encryption key used by the algorithms internally in the user device result in a successful authentication, the encryption key is replaced with another key of a different level.